UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,625	06/18/2001	Jacob Joel Faul	CARDIFF.047A	1239

20995 7590 03/14/2006

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/883,625	FAUL, JACOB JOEL	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 03 January 2006 has been noted and made of record.

2. Claims 1-23 have been presented for examination.

Response to Arguments

3. Applicant's arguments filed 03 January 2006 have been fully considered but they are not persuasive.

4. In response to the Applicant's argument that the prior art of record fails to disclose wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction, the Examiner disagrees. At column 5, lines 12-24, Robinson discloses that the encryption step is used primarily for the purpose of verification [of the transaction] by the merchant. Further down column 5, at lines 41-52, Robinson discloses that the merchant uses a public key cryptosystem where the customer may obtain a public key to decrypt the transaction receipt, thereby providing an opportunity for the customer to verify the transaction.

5. In response to applicant's argument that Robinson does not disclose decrypting the transaction receipt by the second party to prove the transaction, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

6. The Applicant is reminded that patents are relevant as prior art for all they contain. The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art,

relevant for all they contain. See MPEP 2123; see also *In re Heck*, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill in the art, including non-preferred embodiments. See *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied*, 493 U.S. 975 (1989); see also *Celeritas Technologies Ltd. v. Rockwell International Corp.*, 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998).

7. In response to applicant's arguments, the recitation authentication by a third party has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

8. See further rejections below.

Claim Rejections

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 4, 5, 8, 15, 18, 20, and 22 are rejected under both 35 U.S.C. 102(a) and 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,915,022 to Robinson et al., hereinafter Robinson.

11. As per claims 4 and 20, Robinson teaches a method of verifying a transaction conducted between a first party and a second party, the method comprising:

receiving transaction elements of the transaction (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

identifying at least a portion of the received transaction elements as selected elements (Figures 3b, 3c, column 4, lines 34-65, i.e. identifying confirmation number, customer name, date, description of transaction, etc.);

attaching at least a portion of the received transaction elements to a certificate template (Figures 1-2 [step 118], 2 [block 118a], column 4, lines 34-65, column 6, lines 23-48, i.e. transaction record is encrypted and appended to a message, the encrypted transaction record is appended to the digital receipt page);

encrypting the selected elements based on a private key of the first party to generate an encrypted code (Figures 1-2 [step 118], 2 [block 118a], column 4, lines 34-65, column 5, lines 41-53, column 6, lines 23-48, i.e. transaction record is encrypted and appended to a message, customer obtains merchant public key can decrypt transaction receipt, the encrypted transaction record is appended to the digital receipt page);

attaching the encrypted code to the certificate template to produce a transaction certificate (Figures 1-2 [step 118], 2 [block 118a], column 4, lines 34-65, column 6, lines 23-48, i.e. transaction record is encrypted and appended to a message, the encrypted transaction record is appended to the digital receipt page);

transmitting the transaction certificate with the encrypted code to the second party (Figure 1-2 [step 120], column 6, lines 23-48); and

instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate decrypted selected elements (column 5, lines 41-53, customer obtains merchant public key can decrypt transaction receipt),

wherein the decrypted selected elements are used by the second party to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

12. As per claim 15, Robinson teaches a method of verifying a transaction conducted between a first party and a second party, the method comprising:

transmitting transaction elements of the transaction to the first party (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

receiving a transaction certificate that includes an encrypted code (Figure 1-2 [step 120], column 6, lines 23-48);

retrieving a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt); and

decrypting the included encrypted code based on the retrieved public key of the first party to generate decrypted proof elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt),

wherein the decrypted proof elements are used to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

13. As per claim 18, Robinson teaches a method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving a transaction certificate with an encrypted code (Figure 1-2 [step 120], column 6, lines 23-48);

retrieving a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt);

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt); and

declaring the transaction between a first party and a second party including the decrypted proof elements as authenticated if the decrypting is successful (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

14. As per claim 22, Robinson teaches a computing device for verifying a transaction conducted between a first party and a second party, the device comprising:

a submitting module configured to submit transaction elements of the transaction from the second party to the first party (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

a receiving module configured to receive a transaction certificate including an encrypted code from the first party to the second party (Figure 1-2 [step 120], column 6, lines 23-48); and

a first decryption module configured to decrypt the encrypted code to generate decrypted proof elements, based on a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt),

wherein the decrypted proof elements are used to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

15. Claims 1-3, 6, 7, 11-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Robinson in view of U.S. Patent No. 6,243,480 to Zhao et al., hereinafter Zhao.

16. As per claim 1, Robinson teaches a method of verifying a transaction conducted between a first party and a second party, the method comprising:

receiving transaction elements of the transaction (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

identifying a portion of the received elements (Figures 3b, 3c, column 4, lines 34-65, i.e. identifying confirmation number, customer name, date, description of transaction, etc.);

transaction elements as selected encrypting the selected elements based on a private key of the first party to generate an encrypted code (column 4, lines 34-65, column 5, lines 41-52, i.e. creating a transaction record/code based on user elements using merchant's own private key);

sending the transaction certificate with the encrypted code to the second party (Figure 1-2 [step 120], column 6, lines 23-48); and

decrypt the encrypted code in electronic form based on a public key of the first party to generate decrypted selected elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt),

wherein the decrypted selected elements are used by the second party to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

17. Robinson does not disclose printing at least a portion of the received transaction elements on a hard copy transaction certificate; printing the encrypted code on the hard copy transaction

certificate; and instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form.

18. Zhao teaches receiving a hard copy of a document with partial authentication information and scanning in the analog reference to convert the encrypted code into an electronic form for verification (column 3, line 57 to column 4, line 14).

19. It would have been obvious to one of ordinary skill in the art to print out a hard copy of the transaction receipt to be scanned in later to verify a transaction, since Zhao states at column 3, lines 41-54 that such a modification would provide a way to authenticate a digital receipt that has been printed out without losing the authentication information.

20. Regarding claims 2, 5, and 10, Robinson discloses prompting the second party to enter transaction elements of the transaction on an electronic transaction document (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

wherein receiving transaction elements comprises receiving transaction elements entered by the second party on the electronic transaction document (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65).

21. Regarding claims 3, 8, and 13, Robinson teaches identifying an element of a current date and time as one of the selected elements (Figures 3b, 3c, column 4, lines 34-65, column 5, lines 53-64).

22. Regarding claims 6 and 11, Robinson does not disclose wherein transmitting the transaction certificate comprises sending the transaction certificate to an email address of the second party.

23. Zhao teaches transmitting the sending the transaction information to an email address of the second party (column 14, line 57 to column 15, line 17).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit the digital receipt via email, since it is well known that email provides for an easy and inexpensive method to transmit information over a network.

25. Regarding claims 7 and 12, Robinson discloses using URLs to send the digital receipt back to the consumer.

26. Robinson does not teach transmitting the URL to an email address of the second party.

27. Zhao teaches transmitting the sending the transaction information to an email address of the second party (column 14, line 57 to column 15, line 17).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit the URL of the digital receipt via email, since it is well known that email provides for an easy and inexpensive method to transmit information over a network.

29. As per claim 14, Robinson discloses a method of verifying a transaction conducted between a first party and a second party, the method comprising:

identifying a portion of transaction elements of the transaction (Figures 3b, 3c, column 4, lines 34-65, i.e. identifying confirmation number, customer name, date, description of transaction, etc.);

transmitting transaction elements of the transaction and the identification of the transaction elements to the first party (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

retrieving a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt); and

decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt),

wherein the decrypted proof elements are used to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

30. Robinson does not teach receiving a hard copy transaction certificate that includes an encrypted code; and scanning the received transaction certificate to convert the encrypted code to electronic form.

31. Zhao teaches receiving a hard copy of a document with partial authentication information and scanning in the analog reference to convert the encrypted code into an electronic form for verification (column 3, line 57 to column 4, line 14).

32. It would have been obvious to one of ordinary skill in the art to print out a hard copy of the transaction receipt to be scanned in later to verify a transaction, since Zhao states at column

3, lines 41-54 that such a modification would provide a way to authenticate a digital receipt that has been printed out without losing the authentication information.

33. As per claim 17, Robinson teaches a method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

retrieving a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt);

decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt); and

declaring the transaction between a first party and a second party including the decrypted proof elements as authenticated by the third party if the decrypting is successful (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

34. Robinson does not teach receiving a hard copy transaction certificate with an encrypted code by a third party; and scanning the received transaction certificate to convert the encrypted code into electronic form.

35. Zhao teaches receiving a hard copy of a document with partial authentication information and scanning in the analog reference to convert the encrypted code into an electronic form for verification (column 3, line 57 to column 4, line 14).

36. It would have been obvious to one of ordinary skill in the art to print out a hard copy of the transaction receipt to be scanned in later to verify a transaction, since Zhao states at column

3, lines 41-54 that such a modification would provide a way to authenticate a digital receipt that has been printed out without losing the authentication information.

37. Claims 9, 10, 16, 19, 21, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Robinson in view of U.S. Patent No. 6,285,991 to Powar, hereinafter Powar.

38. As per claims 9 and 21, Robinson teaches a method of verifying a transaction conducted between a first party and a second party, the method comprising:

receiving transaction elements of the transaction (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

identifying at least a portion of the received transaction elements as selected elements (Figures 3b, 3c, column 4, lines 34-65, i.e. identifying confirmation number, customer name, date, description of transaction, etc.);

attaching at least a portion of the received transaction elements to a certificate template (Figures 1-2 [step 118], 2 [block 118a], column 4, lines 34-65, column 6, lines 23-48, i.e. transaction record is encrypted and appended to a message, the encrypted transaction record is appended to the digital receipt page);

encrypting the selected elements based on a private key of the first party to generate an encrypted code (Figures 1-2 [step 118], 2 [block 118a], column 4, lines 34-65, column 5, lines 41-53, column 6, lines 23-48, i.e. transaction record is encrypted and appended to a message, customer obtains merchant public key can decrypt transaction receipt, the encrypted transaction record is appended to the digital receipt page);

attaching the encrypted code to the certificate template to produce a transaction certificate (Figures 1-2 [step 118], 2 [block 118a], column 4, lines 34-65, column 6, lines 23-48, i.e. transaction record is encrypted and appended to a message, the encrypted transaction record is appended to the digital receipt page);

instructing the second party to decrypt the included encrypted code based on a public key of the first party to generate decrypted selected elements (column 5, lines 41-53, customer obtains merchant public key can decrypt transaction receipt),

wherein the decrypted selected elements are used by the second party to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

39. Robinson does not disclose retrieving a public key of the second party; encrypting the transaction certificate based on the retrieved public key of the second party, to generate an encrypted transaction certificate; transmitting the encrypted transaction certificate to the second party; instructing the second party to decrypt the transmitted encrypted transaction certificate based on a private key of the second party, to produce a decrypted transaction certificate that includes the encrypted code.

40. Powar teaches sending a statement to a customer using the customer's public key system (column 4, lines 55 to column 5, line 17, column 11, lines 1-50). It is known that in public key systems, the public key is available to the public either by the customer or at a centralized location. When someone wishes to send an encrypted communication to the customer, they retrieve the customer's public key, encrypt the communication with the customer's public key, transmit the encrypted message to the customer at which point the customer decrypts the message using the customer's private key.

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the customer's public key to encrypt the transaction certificate for transmission to the customer, since Powar states at column 5, lines 6-17 that such a modification would verify the message as being legitimate, since in the customer is the only one with the private key that could decrypt and read the message.

42. As per claim 16, Robinson discloses a method of verifying a transaction conducted between a first party and a second party, the method comprising:

transmitting transaction elements of the transaction to the first party (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

receiving an encrypted transaction certificate (Figure 1-2 [step 120], column 6, lines 23-48);

retrieving a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt); and

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt),

wherein the decrypted proof elements are used to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

43. Robinson does not teach making a public key of the second party available to the first party; decrypting the received encrypted transaction certificate based on a private key of the second party so as to generate a transaction certificate with an encrypted code.

44. Powar teaches sending a statement to a customer using the customer's public key system (column 4, lines 55 to column 5, line 17, column 11, lines 1-50). It is known that in public key systems, the public key is available to the public either by the customer or at a centralized location. When someone wishes to send an encrypted communication to the customer, they retrieve the customer's public key, encrypt the communication with the customer's public key, transmit the encrypted message to the customer at which point the customer decrypts the message using the customer's private key.

45. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the customer's public key to encrypt the transaction certificate for transmission to the customer, since Powar states at column 5, lines 6-17 that such a modification would verify the message as being legitimate, since the customer is the only one with the private key that could decrypt and read the message.

46. As per claim 19, Robinson discloses a method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

retrieving a public key of the first party (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt);

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements (column 5, lines 47-50, i.e. if a customer obtains the merchant's public key the customer could decrypt the transaction receipt); and

declaring the transaction including the decrypted proof elements as authenticated if the decrypting is successful (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

47. Robinson does not disclose receiving an encrypted transaction certificate; and decrypting the received encrypted transaction certificate based on a private key of the third party so as to generate a transaction certificate with an encrypted code.

48. Powar teaches sending a encrypted statement using a public key system (column 4, lines 55 to column 5, line 17, column 11, lines 1-50). It is known that in public key systems, the public key is available to the public either by the party or at a centralized location. When someone wishes to send an encrypted communication to the party, they retrieve the party's public key, encrypt the communication with the party's public key, transmit the encrypted message to the party at which point the party decrypts the message using the party's private key.

49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the party's public key to encrypt the transaction certificate for transmission to the party, since Powar states at column 5, lines 6-17 that such a modification would verify the message as being legitimate, since the party is the only one with the private key that could decrypt and read the message.

50. As per claim 23, Robinson teaches a computing device for verifying a transaction conducted between a first party and a second party, the device comprising:

a submitting module configured to submit transaction elements of the transaction from the second party to the first party (Figures 1-1 [steps 103, 106], 3b, 3c, column 3, line 60 to column 4, line 14, column 4, lines 34-65);

a second decryption module configured to decrypt the encrypted code based on a public key of the first party to generate decrypted proof elements (column 5, lines 41-53, customer obtains merchant public key can decrypt transaction receipt),

wherein the decrypted proof elements are used to prove the transaction (column 2, lines 31-43, column 6, lines 23-67, column 7, lines 1-33).

51. Robinson does not disclose a receiving module configured to receive an encrypted transaction certificate from the first party to the second party; a first decryption module configured to decrypt the received encrypted transaction certificate, based on a private key of the second party, to generate an decrypted transaction certificate with an encrypted code.

52. Powar teaches sending a statement to a customer using the customer's public key system (column 4, lines 55 to column 5, line 17, column 11, lines 1-50). It is known that in public key systems, the public key is available to the public either by the customer or at a centralized location. When someone wishes to send an encrypted communication to the customer, they retrieve the customer's public key, encrypt the communication with the customer's public key, transmit the encrypted message to the customer at which point the customer decrypts the message using the customer's private key.

53. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the customer's public key to encrypt the transaction certificate for transmission to the customer, since Powar states at column 5, lines 6-17 that such a modification would verify the message as being legitimate, since in the customer is the only one with the private key that could decrypt and read the message.

Conclusion

54. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

55. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

56. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

57. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

58. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
clf

CHRISTOPHER REVAK
PRIMARY EXAMINER
3/9/06